Andersen Consulting

Change History Log:

October 25, 2000 **In Response Reply to: # 01EDU0054S**

Department Of Education
Student Financial Assistance
Carol Seifert
Contracts Office Technical Representative

Subject: Contract # ED-99-DO-0002
Task Order #22.1 CIO Technical Support Team
Deliverable 22.1.5 IT Architecture Framework, Phase I

Dear Ms. Seifert

Enclosed is the IT Architecture Framework, Phase I that is required by the subject task order. Attached are suggested changes from the reviewers. Future revisions are not planned, but the document will be updated as appropriate.

Deliverable 22.1.5 IT Architecture Framework, Phase I

Section in Document	Original Text	Changed to
Exhibit 5-3	Intranet	Added "Intranet" to the list of SFA applications in the new version of the document.
5.8	SFA in committed to the concept of the Virtual Data Center. It is the intention of SFA senior management team to migrate all applications to the VDC in a timely and cost effective manner.	SFA in committed to the utilization of the Virtual Data Center. It is the intention of SFA senior management team to migrate all applications to the VDC in a timely and cost effective manner.
Exhibit 6-2	Formatting suggestions	Incorporated into the new version of the document.
6.2.5	Enable the development of security components.	Enable the development and maintenance of security components.
Exhibit 7-2	Formatting suggestions	Incorporated into the new version of the document.
7.3.1	A digital certificate is a specially coded object that uniquely identifies a site. It contains the site's public key for encryption and the site's identification information such as organization name,	Certificates may be implemented for individual users or for systems such as individual servers. Different classes of certificates can be generated with defined levels of trust. The highest levels of trust are typically used in financial transactions

	expiration date and a digital signature of the issuer. It allows verification of the claim that a specific public key does, in fact, belong to a specific individual. These certificates are used by the settings within browsers and firewalls to either permit or restrict users from accessing or downloading components to their machines. Certificate management and access provide for primary components of information security, including authentication, authorization, encryption and non-repudiation. The digital certificate server will provide authentication, issuance and revocation services, including the capability for future digital signature administration.	and where confidentiality requirements are high. Different types of certificates are required for specific cryptographic protocols such as SSL, S/MIME or IPSEC. The X.509 standards defines the data in a certificate. Certificates are commonly stored in a directory.
7.3.5	Changed section header	Identification and Authentication
7.3.6	Database management systems security services contribute to the protection of information, data and resources in open systems. An information domain is a set of users, their information objects and a security policy. An information domain security policy is the statement of the criteria for membership in an information domain and the required protection of the information objects. These information domains are not bounded by systems or even by networks of systems. The provision of database management system security services includes data security policy management, data security service management, data security mechanism management and data security mechanism support management. The database maintains the user and user groups and controls permissions to all database resources—tables, views, fields and other database objects. Most	Databases maintain the user and user groups and controls permissions to all database resources—tables, views, fields and other database objects. Most databases have their own list of users and groups and the database controls user accesses rights at each level. The provision of database management system security services includes data security policy management, data security service management, data security mechanism management and data security mechanism support management.

	databases have their own list of users and groups and the database controls user accesses rights at each level.	
7.3.7	Non-repudiation provides the means to prove that a digital transaction actually occurred, i.e., some form of electronic receipt. Digital signatures and file integrity checks use strong encryption to protect data integrity and guarantee data authenticity with a reasonable degree of assurance.	Non-repudiation provides validation of the integrity and origination of electronically transmitted information. Digital signatures and file integrity checks may use strong encryption to protect data integrity and guarantee data authenticity with a reasonable degree of assurance.
7.3.8	Host-based intrusion detection focuses on events occurring within a system as reported by the various logs in a system, for example, repeated failed logins, attempts to access or modify certain files, or changes in usage patterns. Firewalls will reduce but not entirely eliminate the risk of unauthorized external access to SFA networks and systems. Intrusion detection systems, the digital equivalent of burglar alarms and alarm messages they produce may be linked into the systems management process. The system will identify what was changed and provide means to undo any damage.	Host-based intrusion detection focuses on events occurring within a system as reported by the various logs in a system, for example, repeated failed logins, attempts to access or modify certain files, or changes in usage patterns. Firewalls will reduce but not entirely eliminate the risk of unauthorized external access to SFA networks and systems. Intrusion detection systems, the digital equivalent of burglar alarms and alarm messages they produce may be linked into the systems management process. The system will identify what was changed and provide file names for a systems administrator to use for system restoration.
7.5.3	Based on the corrective action plans and prioritization, the necessary technologies, policies and procedures will be implemented, with compliance and oversight by CIO management	Based on the corrective action plans and prioritization, the necessary technologies, policies and procedures will be implemented, with compliance and oversight by the business units and CIO staff.
Exhibit 7-3	Formatting suggestions	Incorporated into the new version of the document.